Claims

This listing of claims will replace all prior version and listings of claims in the application:

1 – 11. (Withdrawn)

12. (Presently Amended) A method for generating a digital signature for use as ~~of obtaining~~ a random number for utilization in an application requiring ~~a~~ the random number, the method comprising the steps of:

storing a private key of a public/private key pair within a device;

generating within the device a digital signature using the private key and a digital signature algorithm;; and

~~then using said~~ providing to the application external to the device the generated digital signature as the random number for use by the application ~~in the application~~.

13. (Presently Amended) The method of claim 12, further comprising the step of using the generated digital signature as a random number to safeguard against a replay attack.

14. (Presently Amended) The method of claim 12, further comprising the step of using the generated digital signature to generate a session key for secure electronic communications.

15. (Presently Amended) The method of claim 12, wherein the digital signature is generated within a computer chip within the device.

16. (Presently Amended) The method of claim 15, wherein the computer chip itself includes a random number generator.

17. (Presently Amended) The method of claim 16, wherein the digital signature is generated within the computer chip using a the private key ~~of a public-private key pair~~ and a random number obtained from the random number generator.

18. (Original) The method of claim 17, wherein an elliptical curve digital signature algorithm is utilized to generate the digital signature.

19. (Original) The method of claim 18, wherein the random number generator is directly inaccessible from outside of the computer chip.

20. (Original) The method of claim 18, wherein the random number generator is accessible only by a digital signature circuit.

21. (New) A device for the generation of a digital signature for use as a random number for utilization within an application requiring a random number, the device comprising:

a user interface;

a memory means for the storage of a private key of a public/private key pair;

a digital signal component in communication with the memory means, wherein the digital signal component generates a digital signature using a digital signature algorithm, wherein the generated digital signature is made available as a random number to an application that is external to the device.

22. (New) The device of claim 21, further comprising the step of using the digital signature as a random number to safeguard against a replay attack.

23. (New) The device of claim 21, further comprising the step of using the digital signature to generate a session key for secure electronic communications.

24. (New) The device of claim 21, wherein the digital signature is generated within a computer chip.

25. (New) The device of claim 24, wherein the computer chip includes a random number generator.

26. (New) The device of claim 25, wherein the digital signature is generated within the computer chip using the private key and a random number obtained from the random number generator.

27. (New) The device of claim 26, wherein an elliptical curve digital signature algorithm is utilized to generate the digital signature.

28. (New) The device of claim 27, wherein the random number generator is directly inaccessible from outside of the computer chip.

29. (New) The device of claim 27, wherein the random number generator is accessible only by a digital signature circuit.